International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 4889~4897
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp4889-4897

Secure data aggregation in IoT using efficient-CSDA

Swathi S[1], Yogish H. K.[2]
[1]Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, India
[2]Computer Science and Engineering, Sapthagiri College of Engineering, India

Article Info

Article history:

Received Dec 4, 2018
Revised Apr 27, 2019
Accepted Jun 26, 2019

Keywords:

Data aggregation
E-CSDA
IoT
Security
WSN

ABSTRACT

In recent days, IoT has been widely accepted and WSN (Wireless Sensor network) is being used for variety of the applications such as transportation, medical, environmental, military, it moreover the main aim to deploy the WSN is to collect the data about the given set of phenomena. The common task of WSN is to sense the data and send over the network. Moreover, due to the various purpose such as statistical analysis, the data aggregation is required. However, the when the dynamic network topology is considered, it is considered to be the very difficult task to provide the secure and efficient data aggregation. The main issue here is to ensure the security and accuracy of the data aggregation. Hence, in this research we have proposed an algorithm named as E-SDA (Efficient Secure Data Aggregation) in order to provide the secure data. In this, the algorithm provides the flexibility to detect the dishonest honest through neighbor monitoring. Later, extensive simulation has been done in order to prove the convergence of our algorithm.

Corresponding Author:

Swathi S,
Department of Computer Science and Engineering,
Nagarjuna College of Engineering and Technology,
Devana Halli, Bengaluru, Karnataka, India.
Email: s.swathieswar@gmail.com

1. INTRODUCTION

IoT is nothing but the network of different physical devices that are embedded with the actuators, sensors and connectivity, which allows these things to connect as well as exchange the data. The growth in the IoT devices over the years are enormous, and it has increased almost up to 8.4 billion in 2017, also it has been approximated that by the year 2020,the number of devices will be 30 billion. The market value is estimated to be 7.1 trillion dollar by 2020.IoT extends the connectivity of internet beyond the standard devices such as smartphones, desktop, laptop [1].

By the beginning of the third millennium, from the research as well as the industrial perspective WSNs gained interest [2]. WSN is generally defined as the network of several network devices (these devices are generally known as nodes) that senses and capable of controlling the interaction between the computers and the environment [3]. It can sense as well as communicate the data collected from the environment or field. Wireless Sensing Network enables the novel application. The data gathered is sent via various hops to the sink and through the internet, it is received or viewed by the appropriate user. In recent years, WSNs have become one of the emerging technologies that are being constantly used in several major application such as border surveillance [4], environment monitoring [5], health monitoring [6] etc. to collect the information and to detect any particular event. WSN helps in combining the smart things that helps in gathering the data [7]. The devices that are used in WSN are mainly constrained in memory, processing capability and the power. Sensor nodes that are employed in the field produces huge amount of data sensed from the field. These data are sent from the sensor node to the sink. Moreover, if the sink are far from the particular node in that case the DP (Data Packets) have to travel more this causes the more consumption of power.

The Figure 1 shows the typical diagram of IoT, here at first the sensor nodes senses the data and the data is sent to the sink or base station. Later it sends the data to the IoT cloud. Later, end user or the application can retrieve the data from the IoT Cloud.

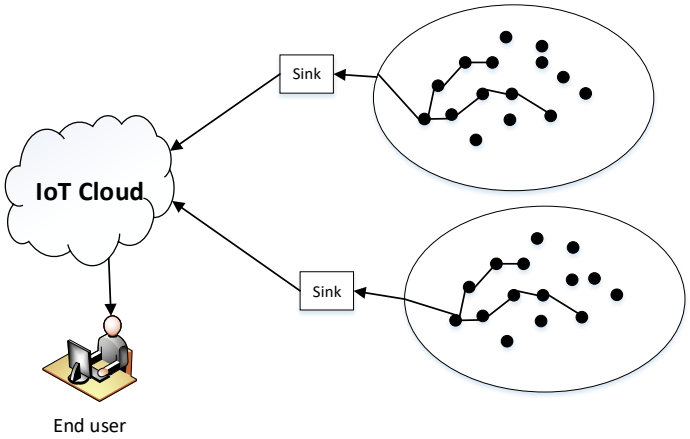

Figure 1. IoT architecture

As a result, a scheme is required to integrate the redundant and correlated data, for that data aggregation is done. The main aim of DA (Data Aggregation) is to maximize the lifetime of a network by minimizing the RC (Resource Consumption) of the nodes [8]. While maximizing the lifetime of a network, there is a possibility that DAP (Data Aggregation Protocols) might reduce the QoS metrics in WSN, these includes absolute data, latency, security and fault-tolerance. Hence designing , developing and maintaining the EDA (Efficient Data Aggregation) is eminent .In various application, the data aggregation is one of the fundamental and basic operation to gather the eminent data . However, just like the other WSNs protocol, even the DA should satisfy the criteria of security. WSNs are very much vulnerable due to their nature of being resource constraint and wireless. This property makes the ideal medium for the attacker to attack the system. The problem becomes more complicated and perplexed, when this occurs in the physical phenomenon. In order to achieve the secure data aggregation (SDA), various cryptographic technique is used such as symmetric and asymmetric key cryptography [9]. However, because of the constraints of the resource, mostly SKC (Symmetric key cryptography) is preferred over the ASKC (Asymmetric key cryptography) However, these techniques requires either the trustworthy authority or the keys technique. To apply the above technique for the large WSN is not at all desirable since it is very much complicated and expensive as well. Hence, it is essential to provide the secure data aggregation.

In order to provide the SDA, we have proposed an algorithm Efficient-CSDA (Consensus based secure data aggregation). Here by taking the advantage of two technique we design our Efficient-CSDA algorithm. First technique is monitoring the neighbor node and second is expansion of dimension. Our scheme is developed to provide the A-CFA (Absolute Collision Free aggregation) as well as to reduce the DAD (Data Aggregation Delay).

This particular research is organized as follows: In Section 2 we briefly discuss about the previous work in data aggregation whereas Section 3 is all about the contribution of this research whereas Section 4 presents the proposed methodology, similarly Section 4 presents result and shows the comparative analysis of our proposed with the existing system. We conclude our research last section.

2. RELATED WORK

Data aggregation is one of the eminent operation in the sensor network; hence, in the last decade there has been considerable effort to look into the secure data aggregation. At first the fixed CBA (Clustering Based Approach) is described which employs the data aggregation, this approach was to prolong life of sensor network [10]. Here, the DA (Data aggregation) is done at two different levels, both of them uses the virtual backbone. In order to increase the lifetime of a network, two algorithms are introduced namely exact and approximate. These two algorithm are used for selecting the master aggregator. Apart from being scalable as well as faster, the AA (approximate approach) gives the outcome, which is nearer to the optimal solution. However, both of the algorithm was applicable only for the certain type of network. To get rid of the network issue, a novel DWS (Deterministic Weighted Sampling) algorithm is presented. DWS is simple

and it is designed to work on any random network topology [11], moreover it is done by introducing various weights for sampling and later updating these weights dynamically. The DWS algorithm tries to distribute the aggregation work on all over sensor node, this is done by enabling every node to create a FSS (Fixed Size Sample). However, the problem with DWS was that the connection loss in the ATS (Aggregation Tree structure) causes the drastic effects. Later, in order to achieve the EEA (Energy Efficient Aggregation) in WSN, an algorithm based on the weighted average operator and fuzzy numbers is presented [12]. Here, the job of algorithm was to minimize the message sent and the message received without influencing the AEQ (Aggregate Estimation quality).However, while performing the algorithm the ratio was not maintained in ideal manner, this affected the lifetime of WSN, and hence in this case the lifetime of WSN was very less. later, the researcher has proposed a scheme of SDA(Secure Data Aggregation) i.e. cluster based in WSN. At first, the CH are chosen based on the connectivity of the given, these nodes act as a Data aggregator. Later, the clustering process takes places and it uses the genetic algorithm. Whenever any cluster member wants to transfer the data, DE (Data Encryption) is utilized. However, it requires large amount of energy and fails to provide the satisfactory security [13].

In [14], SPPDA Scheme is proposed to monitor the system and secure the private data as well, this was mainly based on the bilinear pairing. This system was designed to monitor the health system to improvise aggregation efficiency and secure the data; hence this research formalizes the security model as well as the system model. This paper uses the combination of aggregate signature and Bilinear EIGamal cryptosystem. However, this model has high computational as well as the communication overhead. To improvise the CO(Communication overhead) and computational overhead an efficient as well as secure model is presented [15], this model was mainly based on the ECC (Elliptical Curve Cryptography). This scheme provides fair amount of security and efficiency and tries to achieve the privacy preservation for every data.

Moreover, in [16], along with the parameter of security as well as the privacy concern the several model is compared. By taking the advantage of various schemes, a new scheme is introduced along with the fault tolerance scheme. This scheme aims to provide the computational security along with the minimal communication with the high reliability. Hence, a new efficient method named Laplace DLPA mechanism is introduced; this in terms introduces the low amount of redundant noise. However, the security schemes as well as privacy mechanism are only on the limited resources.

Here, a LPP (Lightweight Privacy Preserving) data Aggregation also known as LPDA is proposed for fog computing [17]. LPDA helps in filtering the false data that are injected by the external attack and supports the efficient aggregate hybrid IoT device and fault tolerance. This methodology is lightweight in both i.e. computation costs as well as Co(Communication Overhead). However, it was limited for the certain devices.

Proposed an algorithm is designed to compute the aggregates such as sum and count, this enables the BS for the verification in case if computed aggregate is valid [18]. The algorithm is known as verification algorithm. The main intention here is to minimize the CO (Communication Overhead) and later the correctness is verified.

In order to save the internal attack [19] proposed a method namely P2DA that is capable of thwarting internal attacks for the given smart grid environment. The described scheme in this research provides the security as well as tries to ensure the lower CC (Communication Costs) other methods have also proposed to protect the privacy and ensure the security such as Fan *et al*. [20] proposed a DA scheme in order to mitigate the internal attacks. However, this method has the weak security. Hence, to enhance this [21] proposed a scheme, which uses the bilinear pairing, but the performance of this method was not up to the mark.

3. CONTRIBUTION OF THIS RESEARCH

SDA (Secure Data Aggregation) has been addressed using the various cryptographic methods. This research mainly focuses on achieving the additive aggregation. Contribution of our research is pointed out below.

a. The aggregation goal is obtained in a distributed way.
b. The initial state of the given node is kept private i.e. not shared by the others, which includes the aggregator as well as the neighbors.
c. The last and one of the eminent contribution of this paper is reduction in Computation as well as communication cost.

4. PROPOSED METHODOLOGY

4.1. System modelling

In this a network model is considered where the given nodes are organized using the clustering algorithm [22]. In our system model, we have considered single connected cluster along with several number of nodes, the main reason behind designing this model is to gather the sensed data from various sensing nodes. In order to make it more flexible we have constructed an overlay network where two nodes can communicate (i.e. exchanging the data) among themselves. The designed overlay network is modeled as the undirected graph. Let's consider any undirected graph$U = (X, Y)$, where X represents the node set and Y represents the edges (link) and B_m be the neighbour set of given node m.

Let $a_m(0)$ be the initial state of any given node in the given network, this initial state represents the private information about each mode. It means that our research primarily focuses on security of node at early state. Our proposed methodology is classified into several section, in first section the GSDA (General Secure Data Aggregation) consensus is introduced which helps us to design our algorithm, next section discuss about monitoring the dishonest or corrupt nodes, third and last section elaborates our proposed algorithm i.e. Efficient-CSDA(Consensus based Data Aggregation) which assures the security.

The Figure 2 shows the flow of our proposed methodology, it basically contains the six stage. First stage is the data collection where the data is collected through the sensor nodes, second stage where the GSDAC (General Secure Data aggregation Consensus) is applied for ensuring the security and adding the noise as well. Third stage is one of the eminent stage where our algorithm allows monitoring the nodes this can be achieved by either through the guidelines or monitoring through the neighboring nodes, However monitoring through the nodes provides more flexibility hence we have considered the second one. At later stage, our algorithm is deployed and the data aggregation takes place securely and it is sent to the Base Station.

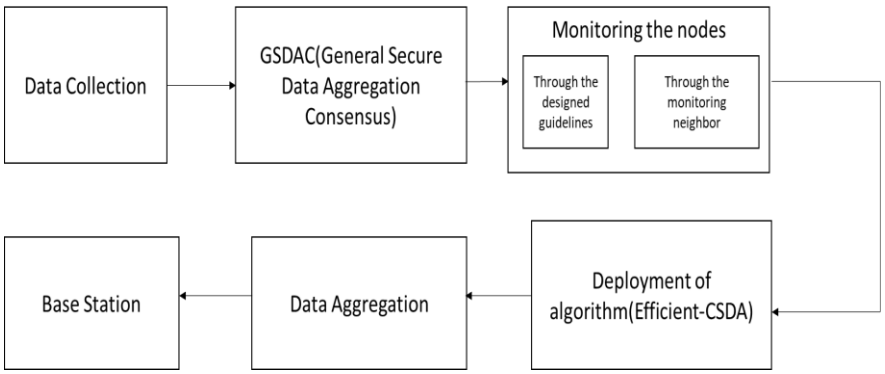

Figure 2. Proposed flow diagram

4.2. General secure data aggregation consensus (GSDAC)

In order to ensure the security, every nodes adds noise to the cotemporary state each time they communicate. Below equation, i.e. Equation (1) presents the noise added.

$$a_m^+(l) = a_m(l) + \theta_m(l), l \in X \quad (1)$$

Here $a_m(l)$ is contemporary stateof node I at iteration I, θ_m represents the noise and it is selected as random variable (RV).

$$a_m(l+1) = V_{mm} a_m^+(l) + \sum V_{mn} a_m^+(l), m \in X, m \in X \quad (2)$$

The Equation (2) represents the updated version of equation 1, V_{mn} is given in Equation (3).

$$V_{mn} = \begin{cases} \frac{1}{[1+\max\{[B_m],[B_n]\}]}, & n \in B_n \\ 1 - \sum_{l \in N_i} V_{mr} & m = n \\ 0, & otherwise \end{cases} \quad (3)$$

The (3) can also be achieved in the distributed manner. The matrix form of the (2) is represented as in (4).

$$a(l+1) = V(a(l) + \theta(l)) \tag{4}$$

In the above equation, $a, \theta \in P^d, V \in P^{dXd}$ which satisfies a,θ and V in (4).

$$\begin{cases} A = [a_1, a_2, \dots\dots, a_n]^Z \\ \theta = [\theta_1, \theta_{2,\dots\dots\dots}\theta_n]^Z \\ V = [V_{mn}]_{dXd} \end{cases} \tag{5}$$

In order to achieve the perfect average and secure consensus, the discarding of corrupt nodes are needed, this can be achieved by two given generic method.

4.3. Monitoring the dishonest nodes

This section of proposed methodology discuss about the dealing with the dishonest nodes that may cause issue in further aggregation. In order to ensure the security nodes in the network has to be monitored, it can be achieved by given two paradigm, first paradigm is using the dimension expansion. In this, the contemporary states are parted into two distinct parts and these two parts are sent to the Neighbor s*et al*ong with the added noise. Particular guidelines are designed for monitoring the nodes, this in terms identify if there is any misconduct found.

4.4. Monitoring the nodes according to the designed guidelines

Dimension expansion is used to monitor the corrupt nodes. Here at first the nodes are parted into two distinguish part Equation (4) and Equation (5) and later along with the distortion, it is sent to the neighbor nodes.

$$a_m^1(0) = \frac{1}{2}a_m(0) + e_m \tag{6}$$

$$a_m^2(0) = \frac{1}{2}a_m(0) - e_m \tag{7}$$

e_m is selected as random variable from 0 < Y < 1.

4.5. Monitoring through the neighbor node

This is another way of monitoring the corrupt nodes; here the aggregator requests the any particular node to monitor the neighboring node at any time. However in order to monitor few condition has to be satisfy.

Condition 1:

$$|\theta_m^e(l)| \leq \frac{1}{2}\alpha\rho^l, where\ \theta_n^e(l) \text{ is computed by}$$
$$\theta_n^e(l) = a_n^{e+}(l) - [V_{nn}^e a_m^{e+}(l-1) + \sum_{r \in B_n^e} V_{nr}^e\, a_r^{e+}(l-1)] \tag{8}$$

And V_n^r is computed using the Equation (3) for $l \in B^+$.

Condition 2:

$$a_n^+(0) - \widehat{a_n}(0) \leq \frac{5}{4}\alpha\rho$$

If the above condition satisfies, then the node j is else the node j is viewed as the corrupt node.

Condition 3:

$$\frac{a_n^+(0)}{2} - a_n^{e+}(0) \leq \frac{5}{4\alpha\rho}$$

4.6. Efficient-CSDA (Consensus based data aggregation)

Step 1 : Random_Vector_Generation
Step 2 : initialization of $a_m^1(0)$ and $a_m^2(0)$ using the equation
Step 3 : initialization of $a_m^+(0)$ and $a_m^{e+}(0)$
Step 4 : value_transmission of the step3 to their neighbor
Step 5 : in case if the given node m is chosen by aggregator himself for monitoring the neighboring node n, given data is formulated and denoted with e, T_r^e, T_n^e, B_n^e for the given value of e=1 or e=2 and $r \in B_n^e$.

Step 6 : set $\delta_m^e(0) = \theta_m^e(0)$
Step 7 : initializing r=1
Step 8 : while r<MAX_IT_NO do
Step 9 : if the node I is selected, the received value $a_m^e(l-1)$, afterwards the IS (Information set) $M_n^e(l-1)$ is used for monitoring the neighbor node.
Step 10 : report_aggregator (if the node is found to be corrupt)
Step 11 : updation of $a_m^e(l) = B_{mm}^e a_m^{e+}(l-1) + \sum_{r \in B_m^e} V_{mr}^e x_l^{v+}(l-1)$
Step 12 : put $a_m(l) = a_m^1(l) + a_m^2(l)$
Step 13 : random _selection of $\delta_m^e(l)$
Step 14 : set $\theta_m^e(l)$ by formulating $\theta_m^e(l) = \delta_m^e(l) - \delta_m^e(l-1)$
Step 15 : put l= l+1
Step 16 : end_while_loop

In the above proposed algorithm i.e. Efficient-CSDA (Consensus based Secure Data aggregation) initially the MAX_IT_NO (Maximum iteration Number) is given.

5. RESULT AND ANALYSIS

This section of the research presents the performance of our proposed model, our algorithm is evaluated by analyzing the results obtained and later in order to prove the accuracy of our proposed algorithm, the results are compared with the existing algorithm.

5.1. Network energy

Network energy is one of the parameter that is considered in order to evaluate the performance of our proposed method since network energy helps in improving the efficiency. The Figure 3 represents the graphical representation of our proposed scheme .our method is evaluated based on the 4 different scenario i.e. for different malicious nodes. In Figure 3, x-axis shows the simulation time whereas y-axis shows the number of dead nodes. From the graph, it is observed that as the malicious nodes increases the simulation time also increases and accordingly.

5.2. Average number of dead nodes

This is one of the parameter used for the evaluation of our algorithm as presented in Figure 4. Here, four case is considered i.e. when 10%, 20 %, 30 % and 40% malicious nodes are induced. In the Figure 4, x axis presents the malicious nodes and y axis shows the average energy utilized during the process. In here we observe that as the malicious nodes increases, it increases along with the increase in average energy utilization. In case of 10 % malicious node, the average number of dead node is more than 4, whereas in case of 20% malicious nodes the average number of dead node is more than the previous malicious nodes. Moreover, when 30% malicious nodes is induced more than 5 number of nodes are dead. Similarly, when 40% malicious nodes are induced, in average more than 6 number of nodes are dead.

5.3. Throughput

Throughput is nothing but the amount of data that are transmitted successfully, it is one of the key parameter to evaluate the performance of our algorithm. The Figure 5 shows the comparison of existing and proposed system based on throughput parameter. The x axis presents the malicious nodes induced where as y axis shows the throughput achieved. As we observe that the increase in malicious nodes reduces the throughput of the method. However, when compared between the existing and proposed our method performs better. When 10% of malicious nodes are induced, the throughput achieved by the existing system is 0.481 whereas proposed method is 0.555. In case of 20% malicious nodes, the throughput achieved by the existing syste is 0.275 whereas proposed method gives the throughput of 0.3685. Similarly, when 30 % malicious nodes are induced, throughput achieved is 0.205 and proposed method achieves the 0.2501. At last when it comes to the 40% malicious nodes, throughput achieved is 0.1672 and the throughput achieved by propose system is 0.22.

5.4. ROC

RoC curve is generated by plotting the FPR (False Positive Rate) against the TPR (True Positive report) at the given threshold point. TPR is also called as sensitivity, whereas FPR known as false alarm. The FPR is computed as (1-specifity). Hence, this RoC curve ROC Curves is used for evaluating the ML (Machine Learning) techniques. It is also used for the evaluation and computation of various algorithm [23] as shown in Figure 6 to Figure 9.

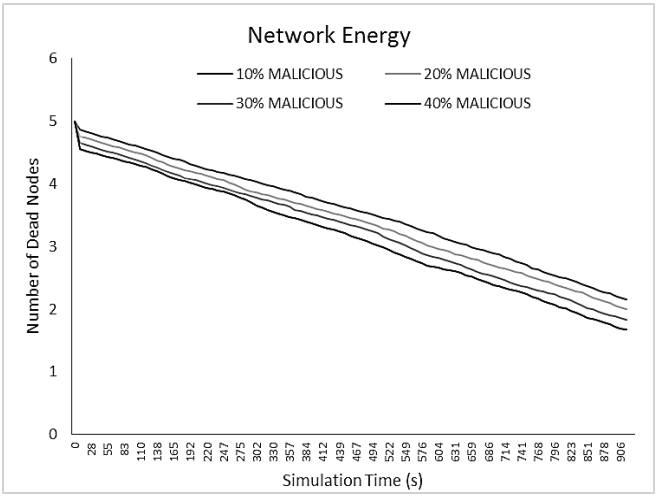

Figure 3. Network Energy

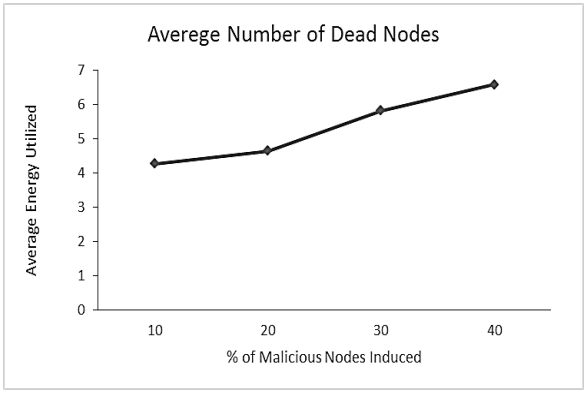

Figure 4. Average number of dead nodes

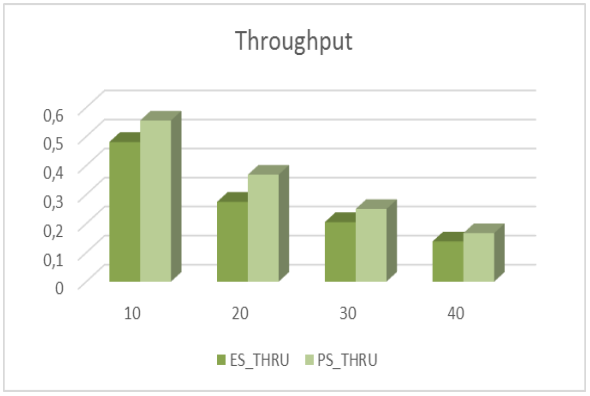

Figure 5. Throughput

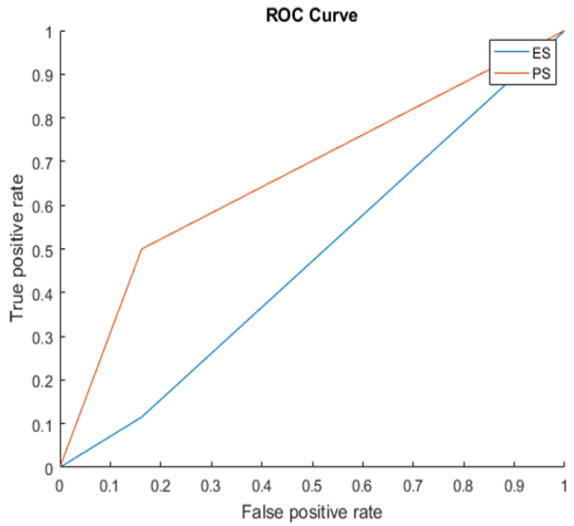

Figure 6. ROC plot for 10 malicious nodes

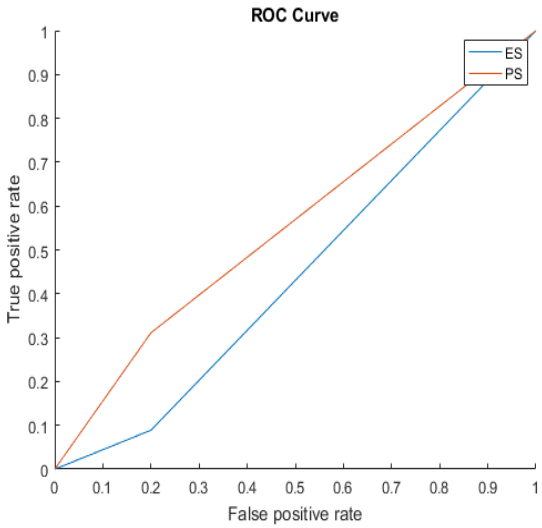

Figure 7. ROC curve for 20 malicious nodes

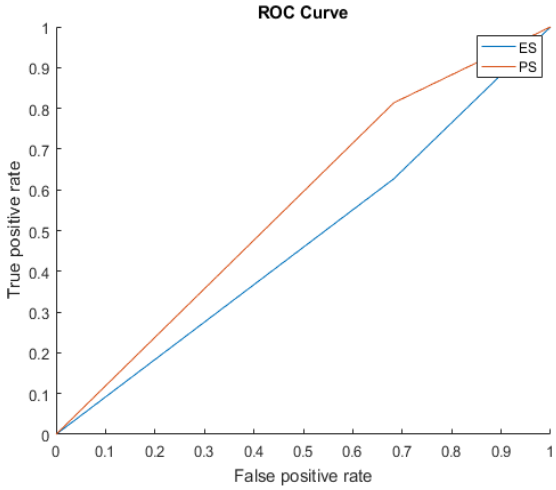

Figure 8. ROC curve for 30 malicious nodes

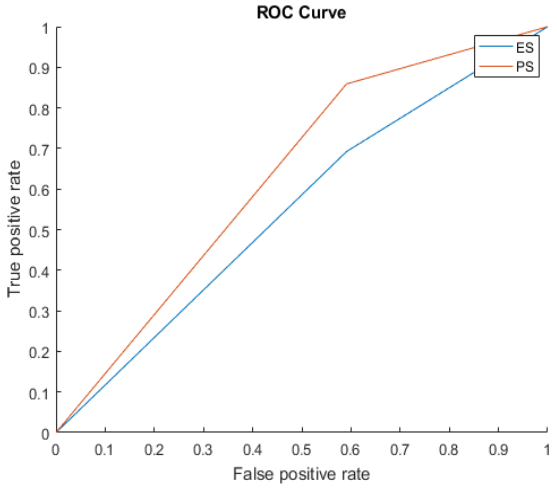

Figure 9. ROC curve for 40 malicious nodes

6. CONCLUSION

Considering the various constraints such as limited energy supply, limited computing capacity and dynamic network topology, it is highly improbable to ensure the secure data aggregation. Hence this research focuses on the distributed SDA (Secure Data Aggregation), it is constructed considering the scenario that dishonest or the corrupt nodes may disrupt or pollute the data aggregation. To get rid of these issue we have proposed algorithm Efficient-CSDA that allows the neighbor to detect the dishonest nodes. In order to evaluate our algorithm, simulation is done based on the various parameter such as throughput, network energy and average number of nodes and it clearly shows that our algorithm excels. Moreover, throughput and network energy is conducted on different malicious nodes i.e. 10%, 20%, 30% and 40% and as the graph in the previous section shows that with the increase in malicious nodes the performance of existing system drops drastically whereas proposed system perform much better. Later the RoC is plotted to evaluate the algorithm and we observe that proposed system performs better than the existing one. Although the performance of proposed system performs much better than the existing one, but still there are several area where investigation is required such as the overlay network has to be undirected as well as directed.

REFERENCES

[1] https://en.wikipedia.org/wiki/Internet_of_things.
[2] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, pp. 375-376, 2014.
[3] V. Potdar, *et al*., "Wireless Sensor Networks: A Survey," *2009 International Conference on Advanced Information Networking and Applications Workshops*, Bradford, pp. 636-641, 2009.
[4] H. Mostafaei, *et al*., "Border Surveillance with WSN Systems in a Distributed Manner," *IEEE Systems Journal*.
[5] T. C. Hoang and C. N. Duy, "Environment monitoring system for agricultural application based on wireless sensor network," *2017 Seventh International Conference on Information Science and Technology (ICIST)*, Da Nang, pp. 99-102, 2017.
[6] U. Gogate and J. W. Bakal, "Smart Healthcare Monitoring System based on Wireless Sensor Networks," *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, pp. 594-599, 2016.
[7] M. Kocakulak and I. Butun, "An overview of Wireless Sensor Networks towards internet of things," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, pp. 1-6, 2017.
[8] M. Ingle and P. V. R. D. P. Rao, "Improving IF Algorithm for Data Aggregation Techniques in Wireless Sensor Networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 5162-5168, 2018.
[9] J. Metan and K. N. N. Murthy, "FSDA: Framework for Secure Data Aggregation in Wireless Sensor Network for Enhancing Key Management," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 4684-4692, 2018.
[10] Rajathi and L. S. Jayashree, "Energy efficient grid clustering based data aggregation in Wireless Sensor Networks," *2016 IEEE Region 10 Conference (TENCON)*, Singapore, pp. 488-492, 2016.
[11] H. Akcan and H. Brönnimann, "A new deterministic data aggregation method for wireless sensor networks," *Signal Processing*, vol. 87, 2007.

[12] B. Lazzerini, *et al*., "A Fuzzy Approach to Data Aggregation to Reduce Power Consumption in Wireless Sensor Networks," *NAFIPS 2006 - 2006 Annual Meeting of the North American Fuzzy Information Processing Society*, Montreal, Que., pp. 436-441, 2006.
[13] L. Bhasker, "Genetically derived secure cluster-based data aggregation in wireless sensor networks," *IET Information Security*, vol. 8, pp. 1-7, 2014.
[14] A. Ara, *et al*., "A Secure Privacy-Preserving Data Aggregation Scheme Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems," *IEEE Access*, vol. 5, pp. 12601-12617, 2017.
[15] O. R. M. Boudia, *et al*., "Elliptic Curve-Based Secure Multidimensional Aggregation for Smart Grid Communications," *IEEE Sensors Journal*, vol. 17, pp. 7750-7757, 2017.
[16] S. Goryczka and L. Xiong, "A Comprehensive Comparison of Multiparty Secure Additions with Differential Privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 463-477, 2017.
[17] R. Lu, *et al*., "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," *IEEE Access*, vol. 5, pp. 3302-3312, 2017.
[18] S. Roy, *et al*., "Secure Data Aggregation in Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1040-1052, 2012.
[19] D. He, *et al*., "Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid Against Internal Adversaries," *IEEE Transactions on Smart Grid*, vol. 8, pp. 2411-2419, 2017.
[20] C. I. Fan, *et al*., "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 10, pp. 666-675, 2014.
[21] D. He, *et al*., "Wireless Netw," vol. 22, pp. 491, 2016. Available: https://doi.org/10.1007/s11276-015-0983-3.
[22] R. Xu and D. Wunsch, "Survey of clustering algorithms," *IEEE Transactions on Neural Networks*, vol. 16, pp. 645-678, 2005.
[23] D. M. W. Powers, "ROC-ConCert: ROC-Based Measurement of Consistency and Certainty," *2012 Spring Congress on Engineering and Technology*, Xian, pp. 1-4, 2012.